Une occasion à saisir : Développer des applis mobiles dans le respect du droit à la vie privée

Introduction

En vertu des lois canadiennes sur la protection des renseignements personnels, toutes les entreprises doivent concilier innovation, esprit d'entreprise et protection efficace des renseignements personnels, et cela s'applique aux concepteurs d'applications mobiles, qu'ils travaillent à leur compte ou pour le compte d'une organisation.

L'environnement mobile, et la nouvelle filière des applications qu'il a créée, ouvrent sans cesse de nouveaux horizons qui évoluent rapidement et qui regorgent de richesses et de possibilités, mais qui présentent également des risques. Par exemple, même si certaines applications comme les nouveaux outils de référence et les jeux font maintenant partie de notre quotidien, on continue de faire état d'accès non autorisés aux renseignements personnels des utilisateurs, notamment les carnets d'adresses, les photos et les données géoréférencées. Conscients de ces développements, les commissaires à la protection de la vie privée du Canada, de l'Alberta et de la Colombie-Britannique ont rédigé ce document d'orientation pour aider les concepteurs d'applications au Canada à tenir compte des caractéristiques uniques de l'environnement mobile qui, selon nous, crée son propre lot de défis inusités pour la protection de la vie privée.

Le premier défi a trait au fait que si l'ère du téléphone intelligent apporte aux consommateurs une connectivité et une commodité sans pareil, le risque de surveillance exhaustive existe bel et bien. L'utilisation récente de capteurs dans les applications, comme celles permettant la localisation, donne la possibilité de suivre nos allées et venues. Si l'on associe ces capteurs à des données sur nos faits et gestes ainsi que sur nos opinions, on peut brosser notre portrait.

Le deuxième défi consiste en la communication d'information pertinente sur les choix en matière de protection des renseignements personnels. Celui-ci ne constitue pas un exercice simple, même dans un environnement de bureautique, et le défi pour les concepteurs d'applications se complique dans l'espace mobile où l'écran est petit et l'attention de l'utilisateur intermittente. En raison de ces caractéristiques de conception, il est encore plus difficile de communiquer aux usagers la bonne information sur leur droit à la vie privée, sous une forme qu'ils peuvent comprendre et au bon moment, pour qu'ils puissent faire des choix éclairés.

Le développement des applications, qui se fait, semble-t-il, à la vitesse de l'éclair, et la possibilité de joindre des centaines de milliers d'utilisateurs dans un laps de temps très court constituent le troisième défi. Comme cette situation évolue rapidement, les commissaires à la protection de la vie privée estiment qu'il est important d'expliquer clairement, et ce, en mode proactif plutôt que réactif, comment les organisations qui développent et lancent des applications mobiles sont tenues de s'acquitter de leurs obligations en vertu des lois sur la protection des renseignements personnels, et de les aider à le faire.

Il importe de prendre conscience de la complexité de l'écosystème des applications mobiles et du nombre d'intervenants qui peuvent avoir accès aux renseignements personnels, notamment les concepteurs, les fournisseurs de services, les plateformes d'applications et les annonceurs. Tous les intervenants ont un rôle à jouer dans la protection des renseignements personnels des utilisateurs d'applications. Le présent document d'orientation cible les concepteurs d'applications : il porte sur la conception et le développement d'applications de même que sur la nécessité de ne jamais perdre de vue la protection des renseignements personnels durant le processus de création. Plus tard, nous pourrons aborder sous un autre angle la protection des renseignements personnels dans les applications.

Préparé conjointement par le Commissariat à la protection de la vie privée du Canada et les commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique, ce document d'orientation veut attirer votre attention sur les principaux aspects du droit à la vie privée à prendre en compte au moment de concevoir et de développer des applications mobiles. On trouvera des sources d'information complémentaires à la fin du présent document.

Faites de la protection des renseignements personnels un avantage concurrentiel de votre produit

Que vous soyez le concepteur d'un jeu populaire accessible gratuitement ou d'une application médicale qui surveille les signes vitaux d'un utilisateur offerte moyennant des frais, à terme, il est dans votre intérêt d'assurer la protection des renseignements personnels. Dans un sondage mené en 2012 auprès d'entreprises canadiennes, 39 % d'entre elles considéraient la protection des renseignements personnels comme un avantage concurrentiel, tandis que 24 % estimaient qu'il s'agissait d'un avantage important. Et elles ont raison : les applications mobiles qui prennent la protection de la vie privée au sérieux seront celles qui sortiront du lot, gagneront la confiance des utilisateurs et mériteront de les fidéliser. Qui plus est, selon l'enquête [en anglais seulement] effectuée en 2012 par le Pew Research Center, 57 % des utilisateurs d'applications aux États-Unis avaient désinstallé une application de peur d'avoir à communiquer leurs renseignements personnels ou ont en fait refusé d'installer une application pour des raisons similaires.

La protection des renseignements personnels peut constituer un avantage concurrentiel important pour les concepteurs d'applications mobiles au Canada. Une étude sur la consommation [en anglais seulement] réalisée en 2012 par l'Association canadienne des télécommunications sans fil a révélé que seulement 22 % des utilisateurs de téléphones intelligents étaient ouverts à l'idée de fournir à un concepteur d'applications des renseignements démographiques ou géoréférencés sur eux-mêmes, afin de recevoir gratuitement une application. Dans le sondage d'opinion publique réalisé par le Commissariat à la protection de la vie privée du Canada en 2011, près des deux tiers des Canadiens (65 %) convenaient que la protection des renseignements personnels allait devenir l'un des enjeux les plus importants avec lesquels le Canada sera confronté au cours des dix prochaines années. Et quelque neuf Canadiens sur dix étaient préoccupés par le fait que certaines entreprises demandent trop de renseignements personnels, ne les protègent pas et les vendent à d'autres organisations. Or, ces résultats montrent que la population canadienne se préoccupe de la protection de la vie privée dans l'espace mobile.

De quelle façon la législation sur la protection des renseignements personnels s’applique-t-elle aux concepteurs d’applications?

En vertu des lois canadiennes sur la protection des renseignements personnels, vous êtes responsable des renseignements personnels recueillis, utilisés et communiqués par l’intermédiaire de votre application. Au niveau fédéral, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) établit des règles de base sur la façon dont les organisations peuvent recueillir, utiliser ou communiquer des renseignements au sujet des personnes dans le cadre d'activités commerciales. La Loi donne aussi aux personnes le droit de consulter les renseignements recueillis à leur sujet par une organisation et de demander qu'ils soient corrigés.

La LPRPDE s’applique aux organisations qui exercent des activités commerciales partout au Canada, sauf dans les provinces du Québec, de l’Alberta et de la Colombie-Britannique, qui ont leurs propres lois sur la protection des renseignements personnels dans le secteur privé[1].

Bien que le présent document d’orientation s’adresse au secteur privé, les concepteurs qui créent également des applications à l’intention de gouvernements, d’organes publics ou de dépositaires de renseignements sur la santé devraient connaître les autres lois sur la protection des renseignements personnels en vigueur au Canada et être en mesure de s’y conformer.

À quoi s’applique la définition de renseignements personnels?

Peu importe le type d’applications que vous développez, vos activités sont probablement visées par l’une des lois canadiennes sur la protection des renseignements personnels, car elles peuvent inclure la collecte, l’utilisation et la communication de renseignements personnels. Par renseignement personnel, on entend généralement de l’information sur une personne identifiable. Les photographies et les adresses de protocole Internet s’avèrent correspondre à la définition dans des cas bien précis, et il existe divers autres types de données recueillies par les applications mobiles qui pourraient être considérés comme des renseignements personnels.

Par exemple, les listes de contacts fournissent des précisions sur les contacts eux-mêmes ainsi que sur les liens sociaux de l’utilisateur. L’authentification biométrique vocale, utilisée par exemple dans les applications de reconnaissance de la voix, nécessite la collecte des caractéristiques qui rendent unique la voix d’une personne. Les données géoréférencées peuvent révéler les habitudes et les modes d’activité des utilisateurs. Quelle que soit la méthode employée pour établir un lien entre un appareil et son propriétaire, qu’il s’agisse d’un identificateur unique de l’appareil ou d’identificateurs multiples reliés, elle permet de combiner les renseignements personnels

pour créer un profil très détaillé et de nature sensible du comportement d'un utilisateur en fonction des circonstances.

La combinaison d'éléments d'information disparates tirés de plusieurs sources peut également donner lieu à des profils détaillés permettant l'identification de personnes. La Cour fédérale a statué que l'information concernerait une personne identifiable lorsqu'il existe une sérieuse possibilité qu'une personne puisse être identifiée grâce à l'utilisation de cette information, seule ou associée à d'autres renseignements disponibles.

Qu'en est-il de l'« activité commerciale »?

Même si vous ne tirez aucun revenu d'une application, il est possible que vous soyez assujetti aux lois canadiennes sur la protection des renseignements personnels[2]. La collecte, l'utilisation et la communication de renseignements personnels en vue d'améliorer l'expérience de l'utilisateur, qui contribue indirectement au succès commercial de votre application, pourraient malgré tout être considérées comme une activité commerciale en vertu de la loi.

Principaux facteurs relatifs à la protection des renseignements personnels à prendre en compte en cas de développement d'applications mobiles

La nature unique des renseignements personnels passant par les appareils mobiles, le défi lié au petit écran et la vitesse du cycle de développement des applications mobiles créent un environnement unique qui souligne le besoin d'assurer une protection complète en matière de vie privée. Dans l'environnement mobile, toutes les parties qui manipulent les renseignements personnels des utilisateurs, notamment les concepteurs, les fournisseurs de services, les plateformes d'applications et les annonceurs, sont tenues de respecter les lois canadiennes sur la protection des renseignements personnels. Les concepteurs, en tant que créateurs des applications, ont une grande incidence sur la vie privée des utilisateurs, soit directement ou par l'entremise de l'entreprise pour laquelle ils travaillent.

1. Vous êtes responsable de votre conduite et de votre code.

En vertu de la législation canadienne sur la protection des renseignements personnels dans le secteur privé, une organisation est responsable des renseignements personnels qu'elle recueille, utilise et communique. La mise en place de bonnes pratiques pour gérer la protection des renseignements personnels n'est pas nécessairement compliquée ou difficile. Tant les entreprises unipersonnelles que les grandes entreprises peuvent mettre en place un programme de gestion de la protection des renseignements personnels, en commençant par désigner une personne responsable de la protection des

renseignements personnels, même si l'équipe est petite.

Le processus d'élaboration d'une politique sur la protection des renseignements personnels vous aidera à passer en revue vos propres pratiques de façon systématique. Quand vous en êtes à l'étape de la planification d'une application, il importe de décrire la collecte, l'utilisation et la circulation des données, ainsi que les politiques en matière de sécurité et de protection des renseignements personnels en vertu desquelles les données sont obtenues et consultées. Ces descriptions doivent être schématisées et évaluées afin d'assurer qu'elles sont conformes à la politique de votre entreprise sur la protection des renseignements personnels

La mise en place de règles de protection de la vie privée au sein de votre entreprise vous aidera à gérer les risques en temps opportun, par exemple les renseignements personnels rendus publics par votre application. Et compte tenu du nombre potentiellement élevé d'utilisateurs de votre application, ces règles vous aideront également à répondre de manière organisée aux demandes d'accès aux renseignements personnels et aux plaintes.

Vous devriez également vous assurer que tous vos accords commerciaux et contrats sont conformes aux lois sur la protection des renseignements personnels, car c'est vous qui, à terme, devrez en rendre compte. Assurez-vous que des contrôles sont en place pour que les tiers traitent les renseignements personnels conformément à leurs obligations en vertu de la loi sur la protection des renseignements personnels, comme dans le cas de l'utilisation des contrats, et assurez-vous que les contrôles répondent aux attentes des utilisateurs.

Vous devriez être prudent quand vous utilisez le code élaboré par un tiers ou une trousse de développement de logiciels – comme celles des réseaux de publicité ou des fournisseurs analytiques – qui pourrait contenir un code dont vous n'avez pas connaissance, comme des maliciels ou des logiciels de publicité insistants.

Pour obtenir de plus amples renseignements sur la responsabilité, consultez le document intitulé *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*, qui a été préparé conjointement par les commissariats à l'information et à la protection de la vie privée de la Colombie-Britannique et de l'Alberta et le Commissariat à la protection de la vie privée du Canada.

2. Soyez ouvert et transparent à propos de vos pratiques en matière de protection des renseignements personnels.

En vertu des lois sur la protection des renseignements personnels, vous êtes tenus d'informer les utilisateurs d'application, de manière claire et compréhensible, de l'usage que vous faites de leurs renseignements personnels. Les utilisateurs exigent de plus en plus que l'on fasse preuve de transparence et récompensent ceux qui agissent correctement en leur accordant leur confiance et en leur offrant leur fidélité.

Les pratiques de développement des applications attirent l'attention

Diverses autorités responsables de la protection des données, des gouvernements et des groupes de défense des consommateurs dans le monde entier s'intéressent de près à la façon dont les applications traitent les renseignements personnels. Les concepteurs d'applications répondent également à la demande de transparence des consommateurs, en leur donnant de l'information et en lançant des applications qui donnent aux utilisateurs un aperçu des données recueillies, utilisées et communiquées à partir de leur appareil par d'autres applications. Plusieurs de ces sources sont énumérées à la fin du présent document.

Avant que les utilisateurs téléchargent votre application

Les utilisateurs ne devraient pas avoir à chercher la politique sur la protection des renseignements personnels de votre application. Ils ont besoin d'une information claire pour évaluer ce que vous entendez faire avec les renseignements les concernant.

Par exemple, dès qu'une application peut être téléchargée, indiquez aux utilisateurs éventuels quels renseignements personnels vous comptez recueillir et pourquoi, le lieu où ils seront stockés (dans le dispositif ou ailleurs), à qui ils seront communiqués et pourquoi, combien de temps vous les conserverez, et formulez toute autre précision utile relative à des questions touchant à la protection des renseignements personnels de l'utilisateur.

Une fois que les utilisateurs ont téléchargé votre application

Vous devriez disposer d'un programme de surveillance pour vous assurer que l'application traite bel et bien les renseignements personnels de la manière décrite dans votre politique sur la protection des renseignements personnels. Et tenez compte des facteurs suivants au cas où vous devriez mettre à jour la politique de protection des renseignements personnels de votre application : informez-en les utilisateurs à l'avance et donnez-leur suffisamment de temps pour fournir de la rétroaction avant de mettre en œuvre les changements. Dites-leur exactement quelles règles vous modifiez de sorte qu'ils n'aient pas à comparer l'ancienne version de la politique avec la nouvelle pour comprendre ce qui se passe.

Si vous modifiez la politique de protection des renseignements personnels de l'application pour inclure de nouvelles utilisations, en particulier des transferts d'information à des tiers, faites en sorte que les changements soient faciles à trouver et à comprendre pendant le processus de mise à jour. Ne passez jamais sous silence les mises à jour des applications qui amoindriront la protection des renseignements personnels de l'utilisateur.

Des avis précis sont requis

Même si la politique de protection des renseignements personnels de votre application informe l'utilisateur de vos pratiques, vous devriez également transmettre des avis précis à l'intention des utilisateurs quand ils doivent décider s'ils consentent à la collecte de leurs renseignements personnels. On trouvera de plus amples renseignements sur la façon d'élaborer des avis pertinents aux sections 4 et 5 du présent document, l'accent étant mis sur l'obtention du consentement sur un petit écran et sur le

bon moment pour transmettre des avis aux utilisateurs.

3. Ne recueillez et ne conservez que les renseignements dont votre application a besoin pour fonctionner, et protégez-les.

Uniquement les renseignements nécessaires

Interrogez-vous sur la question de savoir si vous avez besoin de recueillir des renseignements personnels. Si vous en recueillez, la législation sur la protection des renseignements personnels vous oblige à limiter la collecte aux fins légitimes pour lesquelles ils sont requis. On peut imaginer des cas où les renseignements personnels pourraient être utilisés pour des fonctions supplémentaires d'une application en plus de sa fonction principale. Par exemple, une application pour les enfants qui leur permet d'exercer des compétences de base en mathématiques pourrait recueillir l'adresse électronique des parents pour leur faire parvenir des mises à jour concernant les progrès de leur enfant. Or, un enfant pourrait tout aussi bien résoudre des problèmes d'addition et de soustraction sans fournir aucun renseignement personnel.

Si une application recueille des renseignements personnels, la loi sur la protection des renseignements personnels vous oblige à expliquer pourquoi chaque renseignement est recueilli et comment il est utilisé par votre application. Après, vous serez en mesure d'indiquer aux utilisateurs comment votre application utilise leurs renseignements personnels, pourquoi et les choix qui s'offrent à eux. Revenons à l'exemple de l'application de mathématiques : les parents peuvent choisir de ne pas fournir leur adresse électronique, et renoncer ainsi à suivre les progrès de leurs enfants.

Si vous ne pouvez expliquer le lien entre un renseignement recueilli par votre application et le fonctionnement de celle-ci, vous devriez probablement vous abstenir de recueillir ce renseignement. Par exemple, on ne comprend pas bien pourquoi une application de gestion du temps devrait recueillir l'emplacement ou la date de naissance de l'utilisateur.

Bien que cela puisse être tentant, vous devriez éviter de recueillir des données sous prétexte qu'elles pourraient être utiles par la suite. Les lois canadiennes sur la protection des renseignements personnels vous obligent à limiter votre collecte de données aux fins qui existent déjà et à supprimer les données dont vous n'avez plus besoin pour les fins pour lesquelles elles avaient été recueillies au départ.

La protection des renseignements personnels comporte une caractéristique importante, en matière de renseignements non sensibles, celle de permettre aux utilisateurs de ne pas participer à la collecte de données[3]. De cette façon, si vous partagez avec des tiers (par exemple, un réseau de publicité) de l'information sur le comportement ou des identificateurs d'appareils, votre politique sur la protection des renseignements personnels devrait révéler l'identité de ces tiers et comporter un lien menant à l'information expliquant comment modifier ou supprimer les données. Vous devriez également offrir aux utilisateurs un moyen de ne pas être pisté.

Les applications doivent être conçues de manière à ne pas vous obliger à recueillir des identificateurs propres à un appareil si cette information n'est pas essentielle au fonctionnement de l'application. Évitez d'associer des données d'applications différentes à moins que cette association ne soit évidente pour l'utilisateur et nécessaire. Si vous devez établir des liens, veillez à ce que les données sensibles ne soient pas liées à l'identificateur de l'utilisateur plus longtemps qu'il ne faut.

Par exemple, si votre application transmet des renseignements personnels, vous ne devriez pas les enregistrer à moins que ce ne soit nécessaire. Si vous devez les enregistrer, sécurisez-les et supprimez-les dès que possible.

Évitez de recueillir de l'information sur les déplacements et les activités d'un utilisateur en utilisant des localisateurs et des détecteurs de mouvements à moins qu'ils ne se rapportent directement à l'application et que vous n'ayez obtenu le consentement éclairé de l'utilisateur. N'enregistrez jamais de sons et n'activez pas de caméra intégrée à un appareil sans avoir obtenu l'autorisation expresse de l'utilisateur.

De même, évitez de recueillir des renseignements personnels sur des tiers à partir de l'appareil d'un utilisateur sans avoir obtenu de consentement.

Assurez la sécurité des renseignement recueillis.

Vous devriez avoir mis en place les contrôles appropriés sur l'appareil mobile et les systèmes dorsaux qui stockeront l'information pour assurer la sécurité des renseignements personnels traités. Les mesures de sécurité devraient être adaptées au caractère sensible de l'information. Dans la mesure du possible, les renseignements de l'utilisateur devraient être chiffrés quand ils sont stockés et transmis via Internet.

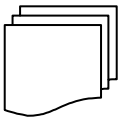
Veillez à ce que les utilisateurs disposent d'un moyen clair et facile de refuser une mise à jour et de désactiver et de supprimer l'application. Vous devriez donner aux utilisateurs la possibilité de supprimer toutes les données recueillies les concernant. En particulier, quand un utilisateur supprime une application, ses données devraient également être supprimées automatiquement.

Pour évaluer si vous êtes prêts à protéger les renseignements personnels, vous pouvez consulter le document intitulé *Protéger les renseignements personnels : Un outil d'auto-évaluation à l'intention des organisations*, qui a été préparé conjointement par les commissariats à l'information et à la protection de la vie privée de la Colombie-Britannique et de l'Alberta et le Commissariat à la protection de la vie privée du Canada.

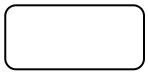
4. Obtenez un consentement éclairé malgré le défi lié au petit écran.

Il y a eu bien des débats sur la nécessité d'améliorer les règles et paramètres de confidentialité sur le petit écran d'un appareil mobile. Le défi consiste à montrer aux utilisateurs, de manière créative et intelligible, à quoi servent réellement les renseignements personnels les concernant. Somme toute, personne ne veut lire 20 pages de politiques sur la protection des renseignements personnels sur un petit écran.

Par conséquent, choisissez la bonne stratégie en matière d'information pour sensibiliser les utilisateurs de l'application sans provoquer une lassitude à l'égard des avis qui fait que les gens ignorent les avis ou les avertissements qu'ils voient trop souvent. Vous pouvez également tirer parti du travail effectué par d'autres sur ce front afin de communiquer de manière efficace les règles de confidentialité sur petit écran. Certains organismes proposent des modèles de politique sur la protection des renseignements personnels pour appareils mobiles et des générateurs, mais vous devez évaluer si les résultats qu'ils affichent vous permettent de vous acquitter de vos obligations en vertu des lois canadiennes sur la protection des renseignements personnels. Voici quelques indices visuels qui peuvent être utiles :



Organisation de l'information en couches : Placez les détails importants au premier plan dans votre politique de protection des renseignements personnels, mais insérez des liens menant aux détails de vos règles de confidentialité de sorte que ceux qui souhaitent de l'information plus détaillée puissent en obtenir. Dès l'entrée en matière, assurez-vous d'attirer l'attention des utilisateurs et d'insister particulièrement sur toute collecte, usage ou divulgation d'information qui dépasse leurs attentes raisonnables.



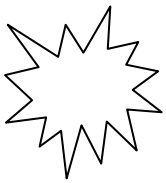
Offre d'un tableau de bord pour la protection des renseignements personnels : Il pourrait aussi être utile d'afficher les paramètres de confidentialité de l'utilisateur à l'aide d'un outil lui permettant de resserrer les paramètres. Cet affichage devrait inciter l'utilisateur à agir, par exemple, en utilisant des boutons radio au lieu de liens hypertextes. Par ailleurs, au lieu de simplement utiliser un bouton mise en marche/arrêt, expliquez aux utilisateurs les conséquences du choix de communiquer des données de sorte qu'ils puissent prendre une décision éclairée. Par ailleurs, veillez à ce que les utilisateurs disposent d'un moyen de modifier leurs renseignements, de renoncer à tout pistage et de supprimer entièrement leur profil s'ils le souhaitent.

Au lieu de simplement utiliser du texte, vous pouvez avoir une politique sur la protection des renseignements personnels plus percutante en utilisant ce qui suit :

Graphique : La première couche de la politique de protection de la vie privée pour votre application mobile pourrait prendre principalement la forme d'icônes, d'étiquettes ou d'images, dans la mesure où ils offrent des liens menant à une information plus détaillée. Vous pouvez également utiliser des graphiques dans l'application au moment où de l'information sensible est sur le point d'être transmise et que le consentement de l'utilisateur est requis. Par exemple, si votre application est sur le point d'accéder aux données géoréférencées de l'utilisateur, vous pourriez activer un symbole afin d'attirer son attention sur ce qui se passe et pourquoi, ainsi que sur les choix qui s'offrent à lui.

Couleur : Vous pouvez éveiller l'attention de l'utilisateur en utilisant

des couleurs et en modifiant leur intensité en fonction de l'importance de la décision ou de la sensibilité de l'information.



Son : L'utilisation sélective de sons et la gradation du volume pour alerter l'utilisateur peuvent aussi être une façon d'attirer son attention sur une décision de protection des renseignements personnels à prendre en temps opportun.

5. Le choix du moment de l'envoi de l'avis à l'utilisateur et de l'obtention du consentement est capital.

La communication avec les utilisateurs à propos de la protection des renseignements personnels dans le contexte des applications mobiles est compliquée par le fait que leur attention dans cet espace est intermittente et limitée. Il est donc important de bien réfléchir et de faire preuve de créativité lorsqu'on décide quand, dans l'expérience de l'utilisateur, les messages sur la protection des renseignements personnels auront le plus d'influence.

Il est important de renseigner les utilisateurs sur les pratiques de confidentialité de votre application au moment du téléchargement et d'obtenir leur consentement. Toutefois, il faut en faire davantage. On ne peut pas s'attendre à ce que les utilisateurs se souviennent des mois plus tard de l'information lue quand ils téléchargent une application, d'autant plus qu'ils en ont de nombreuses sur leur appareil mobile, ce qui limite la valeur de l'obtention d'un consentement ponctuel. Les messages de protection de la vie privée ont plus de poids s'ils sont communiqués au bon moment.

Autrement dit, expliquez aux utilisateurs à l'avance ce qui adviendra de leurs renseignements personnels en cas d'utilisation ou de déploiement de l'application et également en temps réel, au moment où les choses se passent. Sans perdre de vue ce défi en matière de conception, il est crucial que les utilisateurs soient en mesure de faire des choix éclairés au moment opportun. Par exemple, si votre application est sur le point d'avoir activement accès aux données géoréférencées de l'utilisateur, vous pourriez activer un symbole pour attirer son attention sur ce qui se passe. Si votre application prend des photos ou réalise des vidéos, assurez-vous d'indiquer clairement, au moment de prendre la photo ou de tourner la vidéo, que l'application affichera sur l'image les données géoréférencées et qu'elle permettra à l'utilisateur de supprimer cette caractéristique.

Il faudrait attirer l'attention sur les pratiques en matière de protection des renseignements personnels au moment du téléchargement, mais aussi à la première utilisation de l'application. Selon les objectifs de votre application, vous jugerez peut-être utile de donner aux utilisateurs le contrôle des messages à répétition pour éviter qu'ils se lassent des avis, mais ils devraient être en mesure de fixer le délai après lequel le consentement devrait être renouvelé.

Conclusion

Au Canada, par souci de transparence, d'ouverture et de conformité à la loi, on s'attend à ce que les utilisateurs d'applications soient informés des renseignements les concernant qui sont recueillis, utilisés et communiqués et à ce que leur consentement soit éclairé. Compte tenu du succès des applications, vous pouvez vous attendre à un examen plus fouillé des pratiques relatives à la protection des renseignements personnels au sein de votre industrie dans les années à venir – tant de la part des organismes de réglementation que du marché, à l'initiative des consommateurs de plus en plus informés, influents et avisés.

Le présent document d'orientation a été préparé afin de vous aider à améliorer vos pratiques de protection des renseignements personnels et les fonctions de votre application, lesquelles sont cruciales pour aider les utilisateurs à décider des applications auxquelles ils feront confiance et qu'ils continueront d'utiliser. Le respect de ces bonnes pratiques aidera à conforter les utilisateurs dans l'idée que vous avez accordé à la protection de leurs renseignements personnels l'attention qu'elle mérite.

Liste de contrôle : Principaux facteurs relatifs à la protection des renseignements personnels à prendre en compte en cas de développement d'applications mobiles

Vous êtes responsable de votre conduite et de votre code.

- Votre entreprise, qui se résume peut-être à vous seul, est responsable de tout renseignement personnel recueilli, utilisé et communiqué par votre application mobile.
- Assurez-vous d'avoir mis en place des contrôles, comme des contrats ou des contrats d'utilisation, pour faire en sorte que les tiers ayant accès aux renseignements personnels par l'entremise de votre application respectent leurs obligations en matière de protection des renseignements personnels.
- Déterminez la destination des renseignements et recensez les risques applicables à la protection des renseignements personnels.

Soyez ouvert et transparent à propos de vos pratiques de protection de la vie privée.

- Élaborez une politique de protection de la vie privée qui informe les utilisateurs, dans un langage simple, de l'utilisation que fait votre application de leurs renseignements personnels.
- Affichez une politique de protection de la vie privée que les utilisateurs pourront facilement trouver et qui sera facilement accessible aux utilisateurs éventuels qui envisagent de télécharger votre application.

- Ayez en place un programme de surveillance pour garantir que les renseignements personnels sont traités de la façon décrite dans votre politique de protection de la vie privée.
- Quand vous mettez à jour une application, informez les utilisateurs de tout changement à la façon dont leurs renseignements personnels sont traités, et donnez-leur un moyen facile de refuser la mise à jour.

Ne recueillez et ne conservez que les renseignements dont votre application a besoin pour fonctionner, et sécurisez-les.

- Limitez la collecte de données aux fins légitimes pour lesquelles elles sont requises.
- Ne recueillez pas les données en pensant qu'elles pourraient être utiles un jour ou l'autre.
- Permettez aux utilisateurs de refuser une collecte de données qui dépasse celle à laquelle Mettez en place des mesures de sécurité adéquates pour protéger les renseignements personnels que vous traitez. Dans la mesure du possible, utilisez le cryptage lorsque vous stockez et communiquez les données.
- Donnez aux utilisateurs la possibilité de supprimer les renseignements personnels recueillis par votre application. S'ils suppriment l'application, leurs données devraient être effacées automatiquement.

Obtenez un consentement éclairé malgré le défi lié au petit écran.

- Sélectionnez la bonne stratégie pour communiquer les règles de confidentialité de manière efficace sur le petit écran, par exemple :
    - Organisation de l'information sur la protection des renseignements personnels en strates, en plaçant les points importants au premier plan et en proposant des liens menant à des explications plus détaillées.
    - Un tableau de bord pour la protection des renseignements personnels qui affiche les paramètres de confidentialité de l'utilisateur et propose un moyen pratique de les modifier.
    - Des indices visuels comme des graphiques, des couleurs et des sons pour attirer l'attention de l'utilisateur sur l'utilisation qui est faite de ses renseignements personnels, les raisons de cette utilisation et les choix à sa disposition.

Le choix du moment de l'envoi de l'avis à l'utilisateur et de l'obtention du consentement est capital.

- Il faudrait indiquer aux utilisateurs comment leurs renseignements personnels sont traités au moment où ils téléchargent l'application, quand ils l'utilisent pour la première fois et tout au long de leur expérience, pour s'assurer que leur consentement demeure explicite et pertinent.
- Réfléchissez bien et faites preuve de créativité lorsque vous décidez du moment où vous enverrez des messages sur la protection des renseignements personnels afin de trouver le moyen le plus efficace pour retenir l'attention des utilisateurs et avoir le plus d'influence au bon moment, sans causer une lassitude face aux avis. Par exemple, si votre application est sur le point de marquer activement une photo avec les données géoréférencées de l'utilisateur, vous pourriez activer un symbole qui servira de signal à l'utilisateur, lui offrant la possibilité de refuser.

Sources :

Bureaux chargés de la supervision de la protection des renseignements personnels qui ont participé à la rédaction du document

Commissariat à la protection de la vie privée du Canada
Commissariat à l'information et à la protection de la vie privée de l'Alberta (en anglais seulement)
Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique (en anglais seulement)

Mise en œuvre des règles de confidentialité pour votre entreprise

Bureaux de surveillance et organismes gouvernementaux au Canada
Un programme de gestion de la protection de la vie privée : la clé de la responsabilité et *Protéger les renseignements personnels : Un outil d'auto-évaluation à l'intention des organisations* sont des publications conjointes du Commissariat à la protection de la vie privée du Canada et des commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique.
Le Commissariat à la protection de la vie privée du Canada a élaboré plusieurs outils qui seront utiles aux organismes pour apprendre l'essentiel de la protection de la vie privée et de la législation sur la protection des renseignements personnels. Mentionnons entre autres : *Guide à l'intention des entreprises et des organisations – Protection des renseignements personnels : vos responsabilités; Questionnaire sur la protection des renseignements personnels* et une vidéo pour les petits et moyens organismes intitulée *Protégez la vie privée de vos clients : la LPRPDE pour les entreprises*.
Le Commissariat à l'information et à la protection de la vie privée de l'Alberta a rédigé les documents suivants, qui seront utiles : *Guide for Businesses and Organizations on the Personal Information Protection Act*; *Information Privacy Rights*; et *10 Steps to Implement PIPA* (en anglais seulement).
Le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique a élaboré des outils similaires se rapportant à la législation provinciale applicable au secteur privé, notamment : *What are My Organization's Responsibilities Under PIPA?* et *A Guide for Business and Organizations to BC's Personal Information Protection Act* (en anglais seulement).

Documents d'orientation sélectionnés se rapportant à la protection des renseignements personnels à l'intention des concepteurs d'applications

Berkeley Center for Law & Technology, *Mobile Phones and Privacy* (en anglais seulement), le 10 juillet 2012.
Calo, M. Ryan. Against Notice Skepticism in Privacy (and Elsewhere) (en anglais seulement), 87, Notre Dame Law Review 1027, 2012.
Déclaration commune (en anglais seulement) du vérificateur général de la Californie et des plateformes d'applications mobiles sur la protection des renseignements personnels, février 2012.
Electronic Frontier Foundation, Mobile User Privacy Bill of Rights (en anglais seulement), le 2 mars 2012.
Future of Privacy Forum and the Center for Democracy & Technology, Best Practices for Mobile Applications Developers (juillet 2012) et le site pour les concepteurs d'applications du Future of Privacy Forum.
GSMA, Mobile and Privacy: Privacy Design Guidelines for Mobile Application Development (en anglais seulement), février 2012.

Happtique Draft App Certification Program (en anglais seulement), juillet 2012.
Lookout, Mobile App Advertising Guidelines (en anglais seulement), juin 2012.
OASIS Privacy Reference Management Model (en anglais seulement), Version 1.0 Committee Specification Draft, le 26 mars 2012.
Pew Research Centre, Privacy and Data Management on Mobile Devices (en anglais seulement), septembre 2012.
PrivacyChoice Mobile Resources (en anglais seulement)
TRUSTe Mobile Privacy Solutions (en anglais seulement)
Federal Trade Commission des États-Unis, Marketing Your Mobile App: Get It Right from the Start (en anglais seulement), août 2012.
Rapport du personnel de la Federal Trade Commission des États-Unis, Mobile Apps for Kids: Current Privacy Disclosures are Disappointing (en anglais seulement), février 2012.
National Telecommunications and Information Administration des États-Unis, Privacy Multistakeholder Process: Mobile Application Transparency (en anglais seulement), août 2012.

Communication des règles de confidentialité sur petit écran

Know Privacy policy coding methodology (en anglais seulement)
Privacy Icons (beta — en anglais seulement)

Outils sélectionnés d'évaluation de la protection des renseignements personnels par les applications mobiles

Clueful (en anglais seulement)
LBE Privacy Guard (en anglais seulement)
Lookout Premium
MobileScope (en anglais seulement)

---

[1] Le Nouveau-Brunswick et l'Ontario ont des législations essentiellement similaires à la LPRPDE en ce qui concerne les dépositaires de renseignements sur la santé (4 octobre 2012).

[2] Se reporter à la définition d'« organisation » dans la législation de l'Alberta et de la Colombie-Britannique [ces deux liens sont en anglais seulement].

[3] Voir le Cadre pour le consentement négatif, tel qu'exposé par le Commissariat à la protection de la vie privée dans sa Position de principe sur la publicité comportementale en ligne (Juillet 2012).